

Examples of Methods of Development and Implementation

The actions and procedures described below are examples of methods of implementation of the requirements of 806 KAR 3:230, STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement 806 KAR 3:230.

Assess Risk

The licensee:

A. Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;

B. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

C. Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

Manage and Control Risk

The licensee:

A. Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;

B. Trains staff, as appropriate, to implement the licensee's information security program; and

C. Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

Oversee Service Provider Arrangements

The licensee:

A. Exercises appropriate due diligence in selecting its service providers; and

B. Requires its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

Adjust the Program

The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.